Federal Communications Commission
Washington, D.C. 20554

In the Matter of)
)
)
Petition for Rulemaking and Request for) RM-11771
Emergency Stay of Operation of Dedicated)
Short-Range Communications Service in the)
5.850 – 5.925 GHz Band (5.9 GHz Band))

OPPOSITION TO PETITION FOR RULEMAKING AND REQUEST FOR EMERGENCY STAY OF IEEE 1609 DSRC WORKING GROUP

This reply is respectfully submitted by the IEEE 1609 DSRC Working Group[1], a multidisciplinary group of experts who have developed the IEEE 1609 family of DSRC standards (IEEE Std 1609.0-2013, IEEE Std 1609.2-2016, IEEE Std 1609.3-2016, IEEE Std 1609.4-2016, IEEE Std 1609.12-2016). Of importance to this reply is IEEE Std 1609.2-2016, which specifies DSRC security services. As such, we have longstanding expertise and experience in the questions of security of DSRC communications.

Security and privacy have been fundamental DSRC technical and policy requirements since its inception. IEEE Std 1609.2-2016 is comprehensive and informed by industry best practices and by academic research in cryptography, privacy and anonymization. The standard has been through a series of revisions since 2006, with a thorough review at each revision by the Working Group, by the IEEE Standards Association balloting process, and by industry and academic experts. Notable contributors to IEEE 1609.2 include Russ Housley, the former chair

[1] This document solely represents the views of the IEEE 1609 Working Group and does not necessarily represent a position of either the IEEE or the IEEE Standards Association.

of the Internet Engineering Task Force (IETF); Eric Rescorla, the long-standing chair of the IETF Transport Layer Security (TLS) Working Group; and the late Scott Vanstone, one of the pioneers of Elliptic Curve Cryptography.

As a result, comprehensive security and privacy features are already fully integrated into DSRC technology. They have been demonstrated in the US DOT Safety Pilot Model Deployment (thousands of equipped vehicles) and are being implemented in the US DOT Pilot Deployments in New York City, Tampa, and Wyoming (tens of thousands of equipped vehicles). These features are ready for wide scale deployment and are expected to be part of the forthcoming NHTSA DSRC safety mandate. DSRC standards and performance requirements ensure security over the DSRC communication link, up to the appropriate interface within the vehicle where the manufacturer takes responsibility. The DSRC security and privacy approach is also closely harmonized with the European Cooperative ITS communication system, which is currently being deployed.

DSRC has multiple layers of mechanisms built in to protect privacy. Vehicles sign DSRC messages with certificates that do not contain any personal or vehicle identifiers. To prevent attackers from reconstructing vehicle paths by observing the same certificate in multiple places, vehicles frequently change their certificates, and simultaneously change all other identifiers used for communications, such as source MAC and IP addresses and any temporary identifiers. In addition, the design of the certificate management system includes safeguards against any one person or institution knowing any of the certificates used by any single vehicle, even if there is a corrupt insider at the institution or an institution’s database is breached.

It is important to note that the petition raises no specific issues with the DSRC security and privacy approach. It merely states abstract concerns and attempts to create fear using terms like “zombie car apocalypse.” Furthermore, the petition provides no basis for concluding that

DSRC poses a greater threat than any other communication means. This is a critical point. Even without DSRC, the number of connected vehicles will increase substantially in the coming years. The auto industry is also aggressively addressing cybersecurity issues. For example, the Automotive Information Sharing and Analysis Center (Auto-ISAC) facilitates the exchange of important threat information and countermeasures in real time. The petition also refers to NHTSA's timeline for developing cybersecurity guidance without acknowledging the auto-industry developments that will address cybersecurity on a shorter timeline. Banning the use of DSRC would not reduce threats due to connectivity, because it would not significantly reduce connectivity. The real impact of banning the use of DSRC would be to deny society the significant safety of life benefits of DSRC.

In summary, the assertions the petition raises are unfounded as applied to DSRC. Furthermore, the assertions are not specific to DSRC. Granting the petition would deny the public the safety benefits of DSRC.

In our expert opinion the petition is without merit and should be denied.

Respectfully submitted,

-/s/-

Thomas Kurihara
Chair
IEEE 1609 DSRC Working Group

William Whyte
Vice-Chair
IEEE 1609 DSRC Working Group

Justin McNew
Vice-Chair
IEEE 1609 DSRC Working Group

August 24, 2016